



Securing Your Network

# QualysGuard™

The Managed Vulnerability Assessment Solution

## Prevent Network Intrusions to Ensure Business Continuity

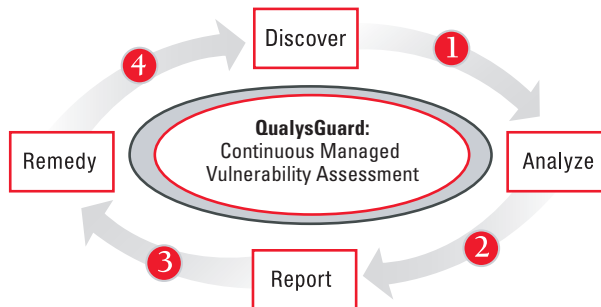
In a climate of increasingly sophisticated and indiscriminate hacker break-ins, every Internet-connected network is a target. The incalculable business costs of compromising corporate Internets, extranets, and intranets makes prevention a top priority for IT organizations of every size. Even for companies that have deployed preventive measures such as firewalls, IDSs, and VPNs, vulnerability assessment has become a critical component of an overall network security strategy.

Identifying and correcting vulnerabilities on network devices and systems before they can be exploited is essential to bulletproof networks against intruders. The issue then: how to secure networks with heterogeneous devices and systems most cost-effectively and with minimal resource demands. The answer: QualysGuard, the Managed Vulnerability Assessment Web service upon which hundreds of network administrators—from Global 2000 enterprises to small business—rely.

## Secure Corporate Data With Continuous Network Auditing

Rather than depend on costly annual audits with penetration testing, network administrators find that QualysGuard's Web service enables them to continuously assess network and system vulnerabilities. There is no hardware or software to install, and no upgrades to maintain, because QualysGuard harnesses the Internet to automatically:

- Reference the most comprehensive and up-to-date vulnerability KnowledgeBase, a CVE-compliant, Qualys™ database tracking thousands of vulnerabilities for more than 300 applications on 20 operating systems, and updated daily as new vulnerabilities emerge.
- Conduct audits with its Inference-Based Scanning Engine, an adaptive process that intelligently runs only tests applicable to the current security profile, from the Qualys library of more than 100 test modules.
- Operate 24x7 and accommodate an unlimited number of scans. Many network administrators pre-schedule routine weekly scans as well as conduct on-demand audits whenever new network devices are introduced or configuration policies change.
- Inventory the entire network of external-facing devices, including upstream routers (ISP entry points), and produce a visual network topology map.
- Scale virtually infinitely with organizations' network growth.



## Identify, Track, and Eliminate Vulnerabilities Before They Are Exploited

The easiest to administer Managed Vulnerability Assessment solution, QualysGuard is a continuous preventive process to:

- Detect network and system vulnerabilities.
- Deliver near-instantaneous email alerts summarizing discovered vulnerabilities and trends.
- Prioritize the severity of each vulnerability on an industry-standard scale, from "watch" to "urgent," so administrators can readily determine where to deploy their security specialists for fixes.
- Recommend and directly link to verified remedies for each vulnerability.
- Produce trend analysis in graphical form, with granular detail appropriate for both security specialists and non-technical management to track vulnerabilities over time.

*"The world of security is becoming more complex and threatening every day. Today, firewalls and intrusion detection solutions simply aren't enough. We need a solution that will not only help us identify potential vulnerabilities, but will also prioritize which vulnerabilities are the most important and what steps are needed to correct them. Qualys has helped companies like ours anchor their security policies with an automated, scalable and proactive solution that will result in a bottom-line ROI."*

Deefay Young  
Senior Network Security Analyst  
Adobe Systems

*"Qualys has been immensely cost-effective in identifying security holes for us. Our security team reviews Qualys' assessment reports and addresses vulnerabilities as quickly as possible, prioritizing fixes according to the level of severity defined by the service. QualysGuard has helped us drastically reduce network vulnerabilities."*

Kevin Ertell  
Director of Internet Technologies and Systems Administration  
Tower Records

# QualysGuard Managed V

## Devices and Applications Scanned by QualysGuard

### Operating Systems:

Windows NT and 2000, Linux, BSD, MacOS X, Solaris, HP-UX, Irix, AIX, SCO, Novell

### Web Servers:

Apache, Microsoft IIS, iPlanet, Lotus Domino, IpSwitch, Zeus; and full support for virtual hosting

### SMTP/POP Servers:

Sendmail, Microsoft Exchange, Lotus Domino, Netscape Messaging Server

### FTP Servers:

IIS FTP Server, WuFTPd, WarFTPd

### Firewalls:

Check Point VPN-1/FireWall-1, Cisco PIX, NetScreen, Gauntlet, CyberGuard, Raptor

### Databases:

Oracle, Sybase, MS SQL, PostgreSQL, MySQL

### eCommerce:

Icat, EZShopper, Shopping Cart, PDGSoft, Hassan Consulting Shopping, Perlshop

### LDAP Servers:

Netscape, IIS, Domino, Open LDAP

### Load Balancing Servers:

Cisco CSS, Alteon, F5 BIG IP, IBM Network Dispatcher, Intel

### Routers, Administrable Switches, and Hubs:

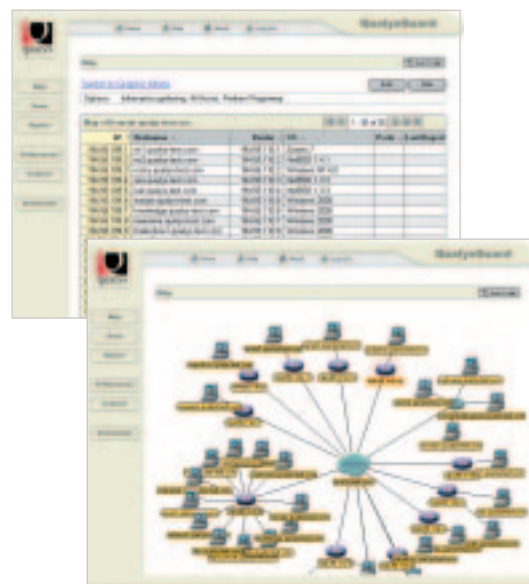
Cisco, 3Com, Nortel Networks, Cabletron, Lucent, Alcatel

## 1. Discover

Dynamic Identification of All Network Perimeter Devices

QualysGuard discovers and creates a visual topology of all of the enterprise's networked devices that can be "seen" from the Internet. By performing full ping sweeps of IP addresses and fingerprinting hosts, QualysGuard accurately characterizes devices, including: access gateways, routers, or other types of equipment; machine types and operating systems; and machine names. Network topology is mapped in graphical and text forms, so administrators can locate devices outside the DNS record as well as validate firewall and IDS configurations.

Subscribers can run pre-scheduled or on-demand network mapping.



## 2. Analyze

Powerful Scanning Engine and Comprehensive, Up-to-Date Database

QualysGuard analyzes each networked device and system for possible vulnerabilities, using a proprietary inference-based methodology that makes no assumptions or eliminations without a complete understanding of the system under test. Inference-based vulnerability scanning assures accurate and complete detection. This includes banner identification and active tests, protocol and daemon fingerprinting, brute forcing and password guessing, and network and application layer testing.

The comprehensive QualysGuard Scanning Engine references a continuously updated Vulnerability KnowledgeBase that includes thousands of network vulnerabilities for over 300 applications, on 20 platforms as well as commercial and open source operating systems, to simulate the "hacker's eye view." Conducted speedily, reliably, and transparently, QualysGuard scanning is non-intrusive—there is no impact on the availability or integrity of the networked devices and systems being scanned. Further, Qualys' technology scales effortlessly to Class C and B size networks.

Subscribers are entitled to an unlimited number of scans, pre-scheduled or on-demand.



# Vulnerability Assessment

## 3. Report

Concise, Actionable Reporting With Trend Analysis

QualysGuard delivers the relevant information to the right people: detailed technical data for IT administrators and easy-to-understand summary data for management, in customizable or pre-defined formats.

### Technical Reporting With Links to Validated Fixes

Graphical reports can be generated in HTML or XML to provide network administrators with a breakdown of the security status of each network device, including summary information about the scan, specific host information, and a list of detected vulnerabilities. These reports present a description of each security risk detected, the severity of the threat (industry standard ratings from 1 to 5), the potential consequences of exposure, and links to validated patches and fixes. Armed with this information, security managers can prioritize where and how to take corrective action.

### Executive Reporting With Trend Analysis

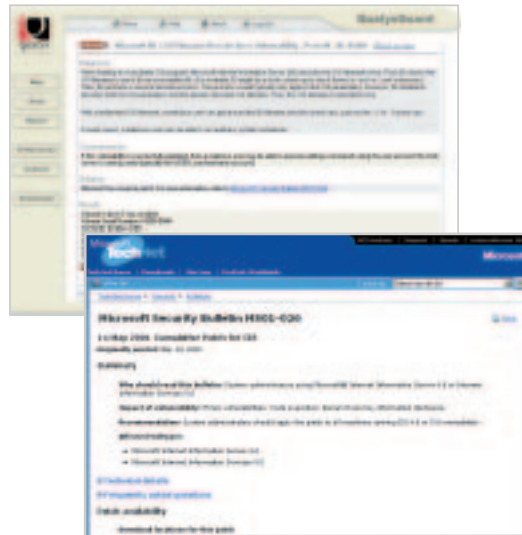
QualysGuard generates graphical management-level reports that provide a global view of the security status of all networks and IP addresses. Based on scanning history, QualysGuard also produces trend analysis and differential reports on security policy compliance. Informed by this global view, executives are better equipped to allocate budgets and update insurers, business partners, shareholders, and boards of directors.

## 4. Remedy

One-Click Links to Verified Fixes

QualysGuard recommends immediate countermeasures, patches, and workarounds for each detected vulnerability. Security experts in Qualys' Vulnerability Laboratory test and validate remedies and provide time-to-fix estimates for vulnerabilities that can be resolved. Qualys customers can verify and document corrected vulnerabilities upon the next QualysGuard scan.

For customers that prefer to outsource vulnerability resolution or require supplemental resources, Qualys has a worldwide network of partners qualified to provide professional services on-site.



## Vulnerability Categories Covered by QualysGuard

- Back Doors and Trojan Horses
- Brute Force Attacks
- CGI
- Databases
- DNS and Bind
- eCommerce Applications
- File Transfer Protocol
- Firewalls
- General Remote Services
- Hardware and Network Appliances
- Information/Directory Services
- SMB/Netbios Windows File Sharing
- SMTP and Mail Applications
- SNMP
- TCP/IP
- Web Servers
- X-Windows

*QualysGuard vulnerability testing is non-intrusive, with no impact on the systems being scanned.*

# QualysGuard Platform

*Automated Network Vulnerability Identification, Elimination, and Verification*

*"Most security solutions, including IDS, function in a reactive mode. We believe that the ideal approach is to have constant, cost-effective, and scalable vulnerability assessment. QualysGuard offers us all of these capabilities in an easy-to-use and automated solution without having to create our own in-house tools."*

Timothy Sanderson  
*eSourcing Manager*  
**Agilent Technologies**

*"With its huge KnowledgeBase of known vulnerabilities and fixes, QualysGuard eliminates the need to hire experts on each of our operating systems and applications... The type of knowledge and recommendations that Qualys offers is invaluable."*

Lenard East  
*Network Engineering and Operations Manager*  
**Bank of the West**



Qualys, Inc.  
1600 Bridge Parkway  
Redwood Shores, CA 94065  
800.745.4355

European Headquarters  
+33 (0) 1 44 17 00 60

[www.qualys.com](http://www.qualys.com)

## QualysGuard APIs

The QualysGuard Application Programming Interface [API] allows Qualys customers and partners to integrate QualysGuard into their own Web service applications. An easy-to-use XML interface facilitates transparent delivery of third-party or in-house security solutions built on essential QualysGuard functions, including:

- Scanning to assess the vulnerability of a host or group of hosts.
- Mapping to identify the topology and characteristics of all hosts under a domain name.
- Enrollment to create new user accounts.

QualysGuard APIs are well documented for easy customization, with working sample code and detailed references to DTDs, Xpaths, XML reports, and sample output.

For more detailed information, please go to <http://www.qualys.com/documentation/api/index.html>.

## QualysGuard Web Service

QualysGuard is the first scalable, affordable Web service providing Managed Vulnerability Assessment for companies of every size. Delivered by subscription over the Internet, QualysGuard employs multiple vulnerability detection techniques with its Inference-Based Engine to assess a network's security exposures and recommend remedies before intruders can take advantage of them. OPSEC-certified QualysGuard for Check Point is also available to monitor VPN-1/FireWall-1 policy changes and detect newly introduced vulnerabilities.

For a free QualysGuard trial, please go to <http://www.qualys.com/forms/trial.html>, email us at [qsales@qualys.com](mailto:qsales@qualys.com), or, in North America, call 800.745.4355.